

What is claimed is:

1 1. A system for performing efficient computer virus scanning of
2 transient messages using checksums in a distributed computing environment,
3 comprising:

4 an antivirus system intercepting an incoming message at a network
5 domain boundary, the incoming message including a body storing message
6 content;

7 a parser module parsing the message content from the body and
8 calculating a checksum over the parsed message content;

9 a checksum module storing the checksum in an information file associated
10 with the incoming message in a transient message store;

11 an antivirus scanner scanning the incoming message for a presence of at
12 least one of a computer virus and malware to identify infected message contents,
13 and recording the checksum corresponding to each infected message content and
14 an infection indicator.

1 2. A system according to Claim 1, further comprising:

2 a message queue enqueueing each incoming message and the associated
3 information file.

1 3. A system according to Claim 1, further comprising:

2 a table of entries, each comprising the checksum and the infection
3 indicator corresponding to each infected message content.

1 4. A system according to Claim 3, further comprising:

2 a comparison module comparing the checksum to the entries in the table
3 prior to scanning operations, and discarding the incoming message if the
4 checksum of the incoming message matches the checksum of one such entry with
5 one such infection indicator.

1 5. A system according to Claim 3, further comprising:

2 a replacement module replacing entries in the table using a least-recently-
3 used replacement algorithm.

1 6. A system according to Claim 3, wherein the table is structured as a
2 binary tree.

1 7. A system according to Claim 1, wherein the checksum is
2 calculated as a running checksum on a line-by-line basis as the incoming message
3 is received.

1 8. A system according to Claim 1, wherein the message content
2 further comprises at least one of an attachment and an embedded attachment.

1 9. A system according to Claim 1, wherein the distributed computing
2 environment is TCP/IP-compliant and each incoming message is SMTP-
3 compliant.

1 10. A method for performing efficient computer virus scanning of
2 transient messages using checksums in a distributed computing environment,
3 comprising:

4 intercepting an incoming message at a network domain boundary, the
5 incoming message including a body storing message content;

6 parsing the message content from the body and calculating a checksum
7 over the parsed message content;

8 storing the checksum in an information file associated with the incoming
9 message in a transient message store;

10 scanning the incoming message for a presence of at least one of a
11 computer virus and malware to identify infected message contents; and

12 recording the checksum corresponding to each infected message content
13 and an infection indicator.

1 11. A method according to Claim 10, further comprising:
2 enqueueing each incoming message and the associated information file
3 onto a message queue.

1 12. A method according to Claim 10, further comprising:
2 maintaining a table of entries, each comprising the checksum and the
3 infection indicator corresponding to each infected message content.

1 13. A method according to Claim 12, further comprising:
2 comparing the checksum to the entries in the table prior to scanning
3 operations; and
4 discarding the incoming message if the checksum of the incoming
5 message matches the checksum of one such entry with one such infection
6 indicator.

1 14. A method according to Claim 12, further comprising:
2 replacing entries in the table using a least-recently-used replacement
3 algorithm.

1 15. A method according to Claim 12, further comprising:
2 structuring the table as a binary tree.

1 16. A method according to Claim 10, further comprising:
2 calculating the checksum as a running checksum on a line-by-line basis as
3 the incoming message is received.

1 17. A method according to Claim 10, wherein the message content
2 further comprises at least one of an attachment and an embedded attachment.

1 18. A method according to Claim 10, wherein the distributed
2 computing environment is TCP/IP-compliant and each incoming message is
3 SMTP-compliant.

1 19. A computer-readable storage medium holding code for performing
2 the method according to Claims 10, 11, 12, 13, 14, 15, 16, 17, or 18.

1 20. A system for performing efficient computer virus scanning of
2 transient messages with message digests, comprising:

3 an antivirus system intercepting an incoming message at a network
4 domain boundary, the incoming message including a header including fields,
5 which each store field values, and a body storing message content;
6 a parser module parsing the field values from each field in the header and
7 the message content from the body;
8 a digest module generating a message digest over each such field value
9 and over the message content and recording the message digests corresponding to
10 the incoming message;
11 an antivirus scanner scanning the incoming message for a presence of at
12 least one of a computer virus and malware to identify infected message contents;
13 and
14 an update module updating the message digest corresponding to each
15 infected message content with an infection indicator.

- 1 21. A system according to Claim 20, further comprising:
2 a message queue enqueueing each incoming message.
- 1 22. A system according to Claim 20, further comprising:
2 a set of digests, each comprising the message digest and the infection
3 indicator corresponding to each infected message content.
- 1 23. A system according to Claim 22, further comprising:
2 a comparison module comparing the message digest to the entries in the
3 table prior to scanning operations, and discarding the incoming message if the
4 message digest of the incoming message matches the message digest of one such
5 entry with one such infection indicator.
- 1 24. A system according to Claim 20, wherein the message content
2 further comprises at least one of an attachment and an embedded attachment.
- 1 25. A system according to Claim 20, wherein the message digest
2 comprises at least one of SHA-1 and MD5 encryption.

1 26. A system according to Claim 20, wherein the bounded network
2 domain is TCP/IP-compliant and each such message packet is SMTP-compliant.

1 27. A method for performing efficient computer virus scanning of
2 transient messages with message digests, comprising:
3 intercepting an incoming message at a network domain boundary, the
4 incoming message including a header including fields, which each store field
5 values, and a body storing message content;
6 parsing the field values from each field in the header and the message
7 content from the body and generating a message digest over each such field value
8 and over the message content;

9 recording the message digests corresponding to the incoming message;
10 scanning the incoming message for a presence of at least one of a
11 computer virus and malware to identify infected message contents; and
12 updating the message digest corresponding to each infected message
13 content with an infection indicator.

1 28. A method according to Claim 27, further comprising:
2 enqueueing each incoming message onto a message queue.

1 29. A method according to Claim 27, further comprising:
2 maintaining a set of digests, each comprising the message digest and the
3 infection indicator corresponding to each infected message content.

1 30. A method according to Claim 29, further comprising:
2 comparing the message digest to the entries in the table prior to scanning
3 operations; and
4 discarding the incoming message if the message digest of the incoming
5 message matches the message digest of one such entry with one such infection
6 indicator.

1 31. A method according to Claim 27, wherein the message content
2 further comprises at least one of an attachment and an embedded attachment.

1 32. A method according to Claim 27, wherein the message digest
2 comprises at least one of SHA-1 and MD5 encryption.

1 33. A method according to Claim 27, wherein the bounded network
2 domain is TCP/IP-compliant and each such message packet is SMTP-compliant.

1 34. A computer-readable storage medium holding code for performing
2 the method according to Claims 27, 28, 29, 30, 31, 32, or 33.

1 35. A system for providing dynamic computer virus and malware
2 protection of message packets in a bounded network domain, comprising:
3 an antivirus system intercepting an incoming message packet, each
4 incoming message packet comprising a plurality of sections comprising a header
5 storing field values and a body storing message packet content, and providing
6 dynamic computer virus and malware protection, comprising at least one of:

7 a checksum module calculating and storing a checksum over the
8 message packet content stored in the body of the incoming message packet; and
9 a digest module generating and storing a digest over at least one
10 the field values stored in the header and the message packet content stored in the
11 body of the incoming message packet;

12 an antivirus scanner scanning the incoming message packet if the at least
13 one of the checksum and the digest have not been previously stored with an
14 infection indicator indicating a presence of at least one of a computer virus and
15 malware.

1 36. A system according to Claim 35, wherein the incoming message
2 packet is discarded if the at least one of the checksum and the digest has been
3 previously stored with an infection indicator indicating a presence of at least one
4 of a computer virus and malware.

1 37. A system according to Claim 35, wherein the distributed
2 computing environment is TCP/IP-compliant and each message packet is SMTP-
3 compliant.

1 38. A method for providing dynamic computer virus and malware
2 protection of message packets in a bounded network domain, comprising:
3 intercepting an incoming message packet, each incoming message packet
4 comprising a plurality of sections comprising a header storing field values and a
5 body storing message packet content;
6 providing dynamic computer virus and malware protection, comprising at
7 least one of:
8 calculating a checksum over the message packet content stored in
9 the body of the incoming message packet; and
10 generating a digest over at least one the field values stored in the
11 header and the message packet content stored in the body of the incoming
12 message packet;
13 storing at least one of the checksum and the digest; and
14 scanning the incoming message packet if the at least one of the checksum
15 and the digest have not been previously stored with an infection indicator
16 indicating a presence of at least one of a computer virus and malware.

1 39. A method according to Claim 38, further comprising:
2 discarding the incoming message packet if the at least one of the
3 checksum and the digest has been previously stored with an infection indicator
4 indicating a presence of at least one of a computer virus and malware.

1 40. A method according to Claim 38, wherein the distributed
2 computing environment is TCP/IP-compliant and each message packet is SMTP-
3 compliant.

1 41. A computer-readable storage medium holding code for performing
2 the method according to Claims 38, 39, or 40.